IN THE CLAIMS

The text of all pending claims, (including withdrawn claims) is set forth below. Cancelled and not entered claims are indicated with claim number and status only. The claims as listed below show added text with underlining and deleted text with ~~strikethrough~~. The status of each claim is indicated with one of (original), (currently amended), (cancelled), (withdrawn), (new), (previously presented), or (not entered).

Please **AMEND** claims 1, 2, 3, 6, 9, 10, 11 and 13-15.

Please **CANCEL** claims 4, 5, 7, 8, and 12.

Please **ADD** new claim 16.

1. (CURRENTLY AMENDED) A cryptographic communication method, comprising: ~~in which a communication key is used for enciphering data to be transmitted in the transmission side, and a key is used for decoding received data in the reception side, wherein in the transmission side~~

individually authenticating, in a transmission side, a communication key and an individual key that is different from the communication key, thereby using both keys ~~is used for enciphering the data to be transmitted~~,

determining, in the transmission side, whether a target file is enciphered by the individual key,

decoding the target file using the individual key, if determined that the target file is enciphered, and not decode processing the target file as an unprocessed target file, if determined that the target file is not enciphered; and

enciphering for transmission, in the transmission side, the decoded target file or the unprocessed target file that is not enciphered, using the communication key, ~~the enciphered data are decoded by using the individual key first, and then the decoded data are enciphered by using the communication key so that the enciphered file can be transmitted~~

wherein in the transmission side, the decoding and the enciphering using the communication key are performed continuously, if the decoding is performed.

2. (CURRENTLY AMENDED) The cryptographic communication method according to claim 1, wherein a file identifier of the ~~original data~~target file is embedded in a file name of the target file, and a new identifier indicating that the ~~data are~~target file is the enciphered ~~data are~~target file, is added to the ~~data~~file name of the target file when enciphering the ~~data~~decoded target file or the unprocessed target file by using the communication key.

3. (CURRENTLY AMENDED) A cryptographic communication method, comprising: ~~in which a key is used for enciphering data to be transmitted in the transmission side, and a communication key is used for decoding received data in the reception side, wherein~~

individually authenticating, in a reception side, a communication key and an individual key that is different from the communication key, thereby using both keys;

decoding, in the reception side, the received ~~data are decoded by~~file using the communication key; ~~, and then the decoded data are enciphered to be memorized by using an individual key that is different from the communication key, and the decoded data are erased~~

determining, in the reception side, whether a target folder for storing the decoded file is for encipher files,

enciphering the decoded file using the individual key and storing the enciphered decoded file in the target folder, if the target folder is for encipher files, and storing the decoded file in the target folder without any encipher processing, if the target folder is not for encipher files,

wherein in the reception side the decoding process and the enciphering process using the communication key are performed continuously, if the enciphering process is performed.

4. (CANCELLED)

5. (CANCELLED)

6. (CURRENTLY AMENDED) A cryptographic communication method, comprising:

authenticating, in a transmission side, an individual key,

~~in which~~authenticating a communication key ~~is~~ that is different from the individual key from among a plurality of communication keys,

~~used for~~ enciphering data to be transmitted in the transmission side from among a plurality of communication keys,

determining, in the transmission side, whether a target file is enciphered by the individual key,

decoding the target file using the individual key, if determined that the target file is enciphered, and not decode processing the target file as an unprocessed target file, if determined that the target file is not enciphered,

enciphering for transmission, in the transmission side, the decoded target file or the unprocessed target file that is not enciphered, using the communication key,

adding an identification code corresponding to the communication key used for the enciphering, and

~~and a communication key is used for decoding received data in the reception side, wherein an identification code corresponding to the communication key used for the enciphering is added to the enciphered data when enciphering in the transmission side, and~~

decoding, in the reception side, the enciphered target file received, from the transmission side, using a ~~the~~ communication key, from among a plurality of communication keys, corresponding to the identification code ~~is used for the decoding~~added in the enciphered target file.

7. (CANCELLED)

8. (CANCELLED)

9. (CURRENTLY AMENDED) A file access system, wherein two different keys are authenticated individually ~~so that they can be used~~, and for data transmission, a decoding process decodes enciphered data stored in an enciphered folder using one of the keys, and an enciphering process automatically enciphers the decoded data for the transmission using the other of the keys ~~are performed continuously for one file~~.

10. (CURRENTLY AMENDED) A file access system, wherein two different keys are authenticated individually ~~so that they can be used~~, and a programmed computer processor controls the file access system according to a process of determining ~~it is decided~~ whether a target file to be transmitted is enciphered, decoding the target file ~~is decoded~~ by using one of the keys, if determined that the target file is enciphered, not decode processing the target file ~~is not processed~~ as an unprocessed target file, if the target file is not enciphered, and for transmission, enciphering the decoded target file or the unprocessed target file using the other of the keys ~~is used for enciphering the unenciphered file~~.

11. (CURRENTLY AMENDED) A file access system, wherein two different keys are authenticated individually ~~so that they can be used~~, and a programmed computer processor control the file access system according to a process of decoding an enciphered file received from a transmission side ~~is decoded~~ by using one of the keys, ~~it is decided~~determining whether a target folder for storing the decoded file is for encipher files, enciphering the decoded file ~~is enciphered~~ by using the other of the keys and ~~is stored~~storing the enciphered decoded file in the target folder, if the target folder is for encipher files, and storing the decoded file ~~is stored~~in the target folder without any encipher process, if the target folder is not for encipher files.

12. (CANCELLED)

13. (CURRENTLY AMENDED) ~~The~~A file access system ~~according to claim 12,~~ comprising a programmed computer processor controlling the file access system according to a process comprising:

displaying a first folder and a second folder,

decoding and/or enciphering a file stored in the first folder when an instruction is input for moving the file from the first folder to the second folder for transmission of the file,

~~wherein it is decided~~determining whether the file stored in the first folder is enciphered,

decoding the file ~~is decoded~~ by using a first key, if determined that the file is enciphered, and not decode processing the file as an unprocessed file, ~~is not processed~~ if determined that the file is not enciphered,

~~and then the unenciphered file is enciphered~~enciphering the decoded file or the unprocessed file by using a second key, and

storing the enciphered decoded file or the enciphered unprocessed file in the second folder for the transmission.

14. (CURRENTLY AMENDED) A computer-readable recording medium on which a program of file access is recorded, the program ~~being for~~ controlling a data transmitting computer ~~to perform the process comprising the steps of~~according to a process comprising:

individually authenticating a communication key and an individual key that is different from the communication key, thereby using both keys; ~~two different keys individually so that they can be used; and~~

determining whether a target file for transmission is enciphered by the individual key;

~~performing a~~ decoding the target file using the individual key, if determined that the target file is enciphered, and not decode processing the target file as an unprocessed target file, if determined that the target file is not enciphered; and

enciphering for transmission the decoded target file or the unprocessed target file that is not enciphered, using the communication key~~process by using one of the keys and an enciphering process by using the other of the keys continuously for one file~~.

15. (CURRENTLY AMENDED) An encipher processing device that is used for a cryptographic communication ~~in which a communication key is used for enciphering data to be transmitted in the transmission side, and a key is used for decoding received data in the reception side~~, the device comprising:

~~the~~a communication key;

an individual key that is different from the communication key; ~~and~~

means for individually authenticating the communication key and the individual key, thereby using both keys;

means for deciding whether a target file is enciphered by the individual key;

means for decoding the target file using the individual key, if the target file is enciphered;

means for enciphering a decoded target file or a target file that is not enciphered, using the communication key; and

means for transmitting the target file enciphered by the communication key;

wherein the decoding process and the enciphering process ~~a process portion for performing a decoding process by using the individual key and an enciphering process by~~ using the communication key are performed continuously, if the decoding process is performed.

16. (NEW) A cryptographic communication method, comprising:

using a communication key for enciphering data to be transmitted by a transmission side, and

using an individual key for decoding enciphered data stored in an enciphered folder at the transmission side,

wherein in the transmission side, the individual key is different from the communication key used for enciphering the data to be transmitted, first, the stored enciphered data are decoded using the individual key first, and, second, the decoded data is enciphered using the communication key for transmission.